Problem Set 4

This problem set is due on *Thursday, October 12* at the end of class.

Each solution is to be handed in *separately*, i.e. on separate sheets of three-hole punched paper. If the solution to a single problem takes more than one page, staple together only the pages relative to the same problem. Mark the top of each sheet with your name, 6.915, the problem number, and the date.

If you collaborate with other students, you MUST write up solutions on your own and acknowledge the people you work with.

NOTE: Because of the holiday, office hours this week will be held on Wednesday October 11 from 4 to 5:30pm in room NE43-344.

Problem 4-1. Logic of Authentication

In this problem we will ask you to apply (a slight modification of) the logic of authentication described in Handout 11 to (a slight modification of) the STS protocol described in Section 5 of the paper *Authentication and Authenticated Key Exchange* contained in Handout 8. In the following assume p to be a large prime, g to be a generator modulo p and all operations being performed modulo p.

The logic that we are going to use is based on the BAN logic of Handout 11. The only differences are the following:

- Assume that the symbols $P \overset{K}{\leftrightarrow} Q$ and $P \overset{K}{\rightleftharpoons} Q$ have the same meaning (P and Q share a key K that can be used for both encryption or authentication)
- Assume that the symbol $\langle x \rangle_k$ means the concatenation of x and $\mathrm{MAC}_k(x)$
- Introduce a new construct $\mathbf{DH}(P, g^x)$: g^x is the Diffie-Hellman public-key of principal P. In particular this means that P knows x.
- Introduce a new deduction rule that we will call the *DH rule* :

$$\frac{P \textbf{ believes } \mathbf{DH}(P, g^x)\ ,\ P \textbf{ believes } \mathbf{DH}(Q, g^y)}{P \textbf{ believes } P \overset{K}{\leftrightarrow} Q}$$

  where $K = g^{xy}$

- Introduce a new deduction rule that we will call the *strong signature rule (SSR)* :

$$\frac{P \textbf{ believes } \overset{PK}{\mapsto} Q\ ,\ P \textbf{ sees } \{x\}_{PK^{-1}}}{P \textbf{ believes } x}$$

Now here is a description of the idealized STS protocol you are going to work with (here $K = g^{xy}$):

$1. A \longrightarrow B : \mathbf{DH}(A, g^x)$
$2. B \longrightarrow A : \mathbf{DH}(B, g^y)\ ,\ \langle\{\mathbf{DH}(B, g^y),\ g^x\}_{PB^{-1}}\rangle_K$
$3. A \longrightarrow B : \langle\{\mathbf{DH}(A, g^x),\ g^y\}_{PA^{-1}}\rangle_K$

We want to prove that

$$A \ \textbf{believes}\ A \overset{K}{\leftrightarrow} B \tag{1}$$

and

$$B \ \textbf{believes}\ A \overset{K}{\leftrightarrow} B \tag{2}$$

The assumptions that we give to begin the analysis are the following

A **believes fresh**(g^x)	B **believes fresh**(g^y)
A **believes DH**(A, g^x)	B **believes DH**(B, g^y)

(a) Prove formally the goals 1 and 2 of the protocol. That is give the complete deductive path as done for Kerberos in Handout 11.

(b) In the above part did you use the fact the messages (2) and (3) are authenticated with MACs? Does the proof goes through even if there is no MAC in those messages, i.e. they become:
2' . $B \longrightarrow A : \mathbf{DH}(B, g^y)\ ,\ \{\mathbf{DH}(B, g^y),\ g^x\}_{PB^{-1}}$
3' . $A \longrightarrow B : \{\mathbf{DH}(A, g^x),\ g^y\}_{PA^{-1}}$

(c) What happens to the proof if we drop both the MACs and the SSR deduction rule? Can you still prove the protocol correct? Or can you find a bug?

Hint: you can find the solution to this question by reading carefully the authentication paper in Handout 8.

(d) (Extra Credit) The original protocol (the one with the MACs) is buggy if we eliminate the SSR deduction rule. Try to find the bug.

Problem 4-2. Passwords

Consider the following scenario: Alice wants to login on a computer system. In order to gain access she has to communicate her password to the system.

However the keyboard (and the cable connection between the keyboard and the system) cannot be trusted since there may be a passive adversary recording the key strokes or tapping the line.

Conversely, let us assume that the display used by Alice (and the connection between the system and the display) is secure, meaning it cannot be monitored by an adversary.

Devise a password protocol that will allow Alice to access the system without disclosing her key to the adversary.